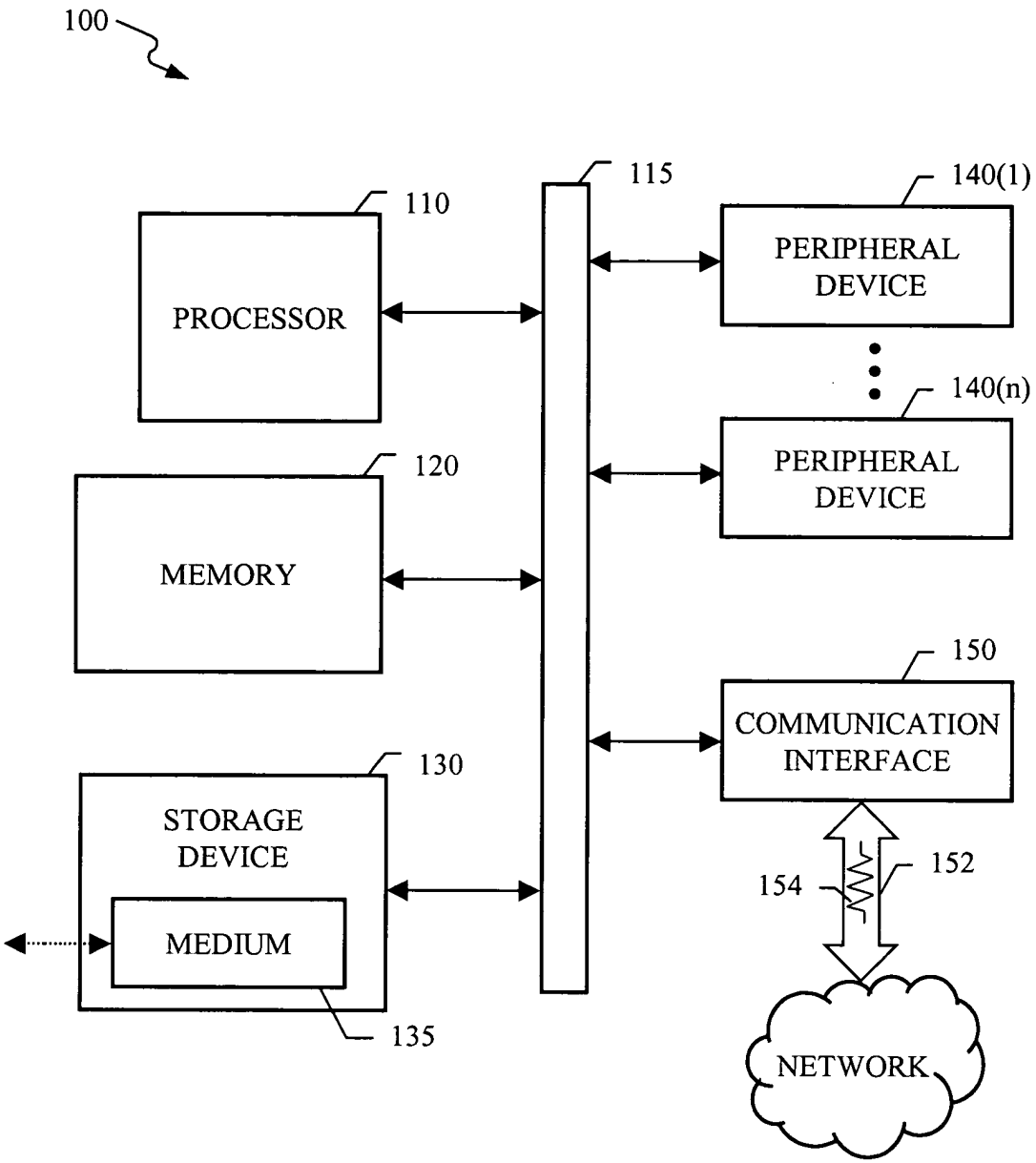
100
115
110
140(1)
PROCESSOR
PERIPHERAL DEVICE
140(n)
120
PERIPHERAL DEVICE
MEMORY
150
COMMUNICATION INTERFACE
130
STORAGE DEVICE
154
152
MEDIUM
135
NETWORK

FIG. 1

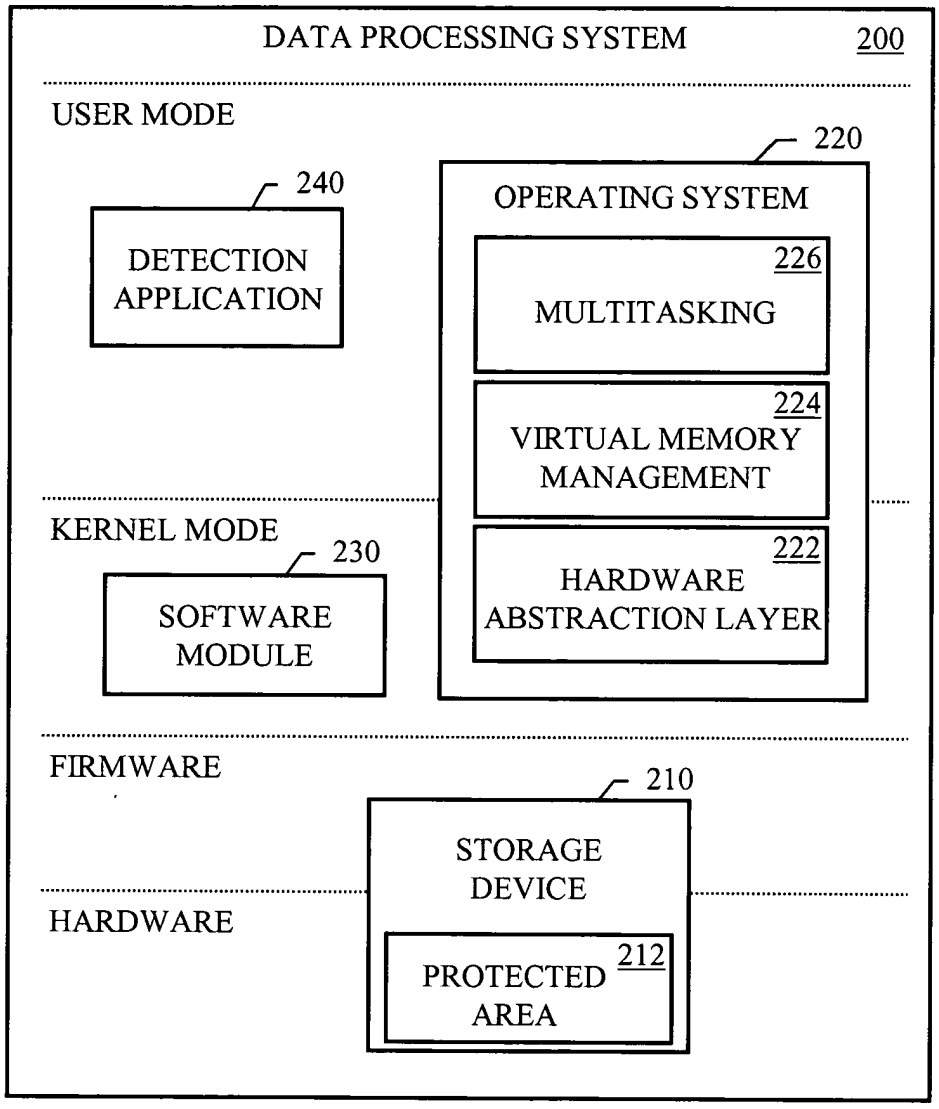
DATA PROCESSING SYSTEM
200
USER MODE
220
240
OPERATING SYSTEM
DETECTION APPLICATION
226
MULTITASKING
224
VIRTUAL MEMORY MANAGEMENT
KERNEL MODE
230
222
HARDWARE ABSTRACTION LAYER
SOFTWARE MODULE
FIRMWARE
210
STORAGE DEVICE
HARDWARE
212
PROTECTED AREA

FIG. 2

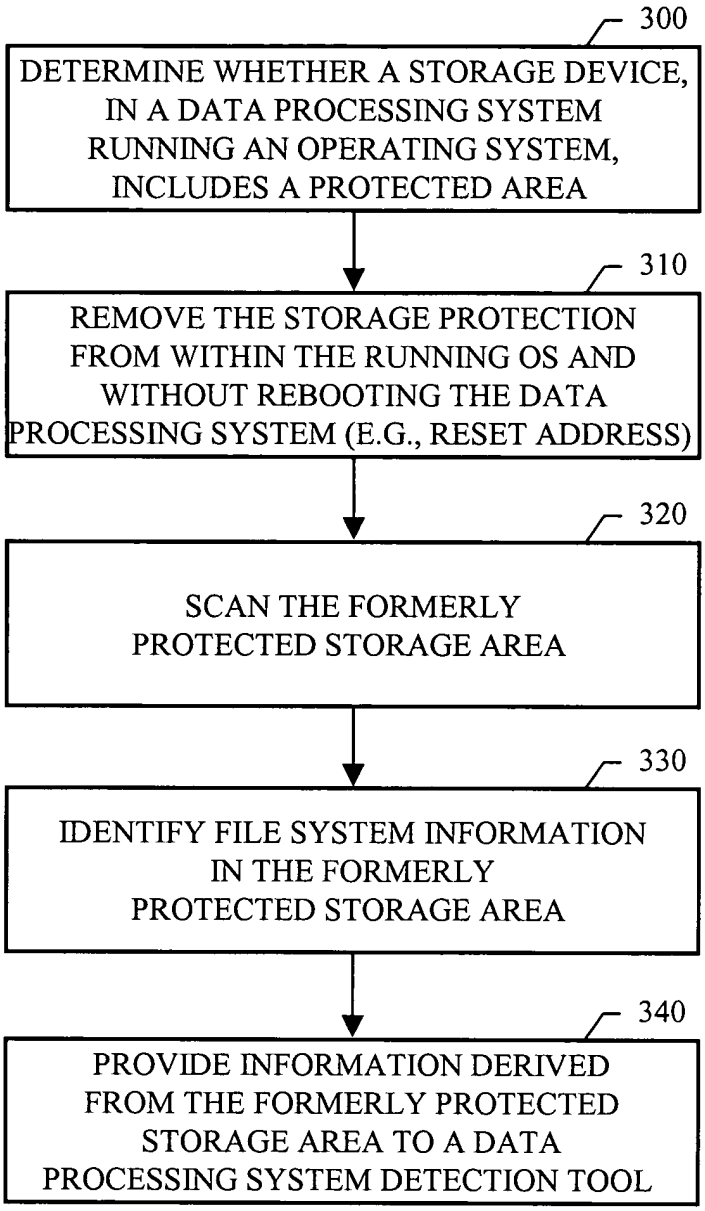
300
DETERMINE WHETHER A STORAGE DEVICE, IN A DATA PROCESSING SYSTEM RUNNING AN OPERATING SYSTEM, INCLUDES A PROTECTED AREA
310
REMOVE THE STORAGE PROTECTION FROM WITHIN THE RUNNING OS AND WITHOUT REBOOTING THE DATA PROCESSING SYSTEM (E.G., RESET ADDRESS)
320
SCAN THE FORMERLY PROTECTED STORAGE AREA
330
IDENTIFY FILE SYSTEM INFORMATION IN THE FORMERLY PROTECTED STORAGE AREA
340
PROVIDE INFORMATION DERIVED FROM THE FORMERLY PROTECTED STORAGE AREA TO A DATA PROCESSING SYSTEM DETECTION TOOL

FIG. 3

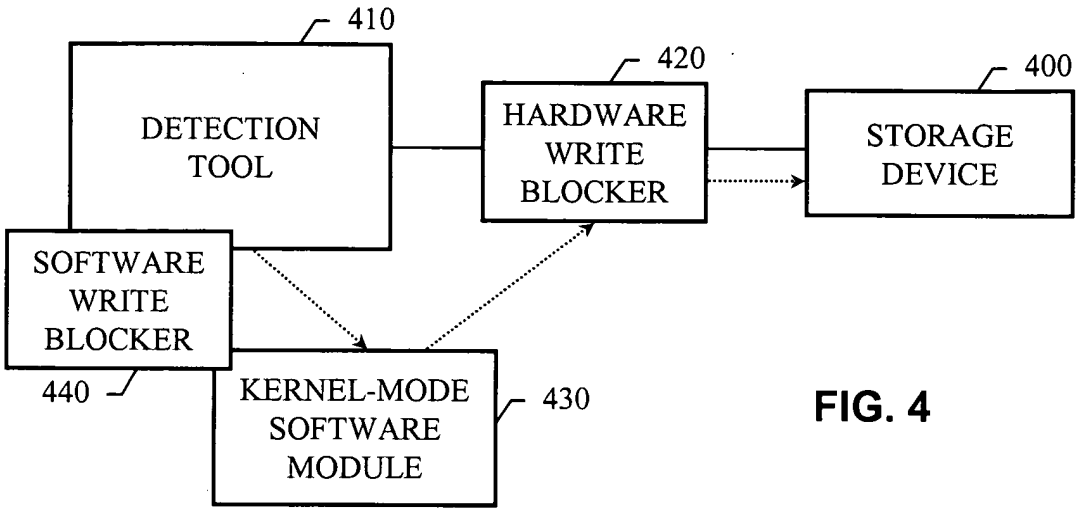
410
DETECTION TOOL
420
HARDWARE WRITE BLOCKER
400
STORAGE DEVICE
SOFTWARE WRITE BLOCKER
440
KERNEL-MODE SOFTWARE MODULE
430

FIG. 4

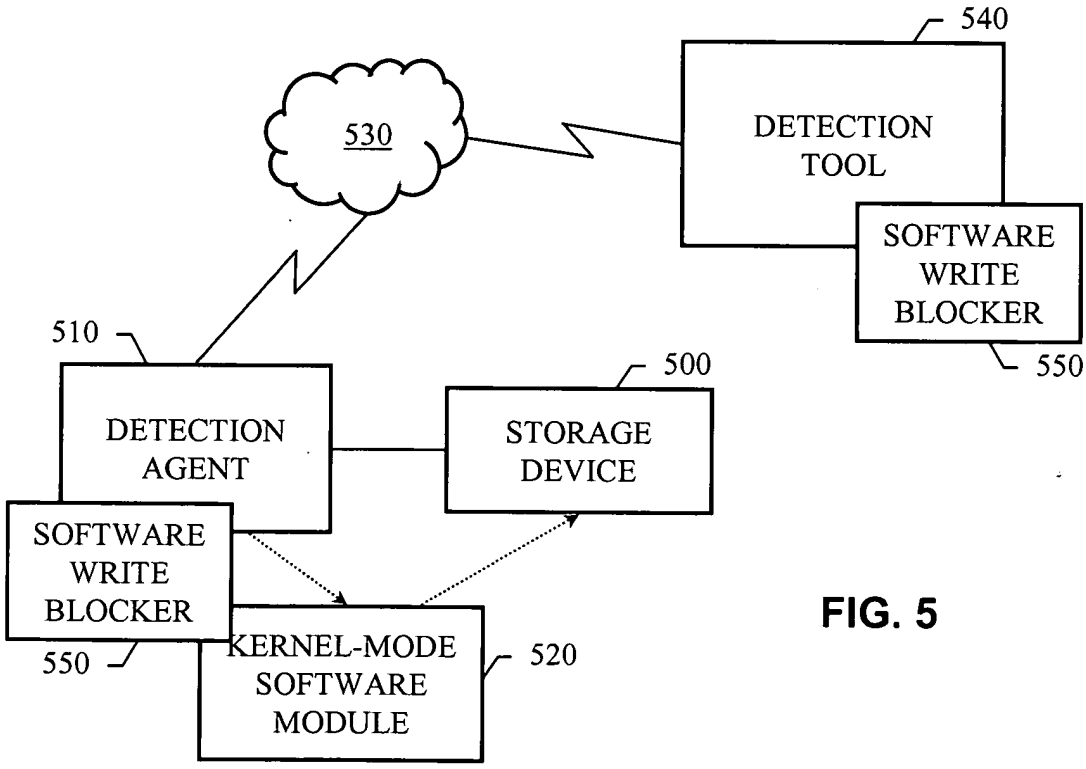
540
530
DETECTION TOOL
SOFTWARE WRITE BLOCKER
550
510
500
DETECTION AGENT
STORAGE DEVICE
SOFTWARE WRITE BLOCKER
550
KERNEL-MODE SOFTWARE MODULE
520

FIG. 5

	Offset	Size in bytes	Data Type
600	0 to 3	4	UINT
610	4 to 42	39	UUID
620	43 – 81	39	UUID
630	82	1	BOOL
640	83 – 97	15	CHAR
650	98 – End of packet		

FIG. 6

	Offset	Size in bytes	Data Type
700	0 to 3	4	UINT
710	4 to -		

FIG. 7

	Offset	Size in bytes	Data Type
800	0 to 3	4	UINT
810	4 to -		

FIG. 8

	Offset	Size in bytes	Data Type	Value
900	0 to 3	4	UINT	PDS_BROADCAST
910	4 to 8	5	BYTE	'PDCLI'
920	9 to 12	4	UINT	
930	13 to 16	4	UINT	
940	17 to		CHAR	

FIG. 9

	Offset	Size in bytes	Data Type	Value
1000	0 to 3	4	UINT	PDS_RES_BROADCAST
1010	4 to 8	5	BYTE	'PDSRV'
1020	9 to 12	4	UINT	
1030	13 to 16	4	UINT	
1040	17 to		CHAR	

FIG. 10

	Offset	Size in bytes	Data Type	Value
1100	0 to 3	4	UINT	PDS_RQ_CONNECT
1110	4 to 42	39	BYTE	
1120	43 to 77	35	BYTE	
1130	78 to 97	20	BYTE	

FIG. 11

	Offset	Size in bytes	Data Type	Value
1200	0 to 3	4	UINT	PDS_RES_CONNECT
1210	4	39	BYTE	

FIG. 12

	Offset	Size in bytes	Data Type	Value
1300	0 to 3	4	UINT	PDS_RQ_SERVER_INFO, PDS_RES_SERVER_INFO
1310	4 to 38	35	BYTE	
1320	39	1	BYTE	
1330	40	4	INT	
1340	44	4	BOOL	

FIG. 13

	Offset	Size in bytes	Data Type	Value
1400	0 to 3	4	UINT	PDS_RQ_HDINFO

FIG. 14

	Offset	Size in bytes	Data Type	Value
1500	0 to 3	4	UINT	PDS_RES_HDINFO
1510	4 to 7	4	DWORD	
1520	8 to 11	4	DWORD	
1530	12 to 15	4	DWORD	

FIG. 15

	Offset	Size in bytes	Data Type	Value
1600	0 to 3	4	UINT	PDS_RQ_PAUNPROTECT
1610	4	1	BYTE	HD num

FIG. 16

	Offset	Size in bytes	Data Type	Value
1700	0 to 3	4	UINT	PDS_RES_PAUNPROTECT
1710	4	1	BYTE	HD num
1720	5	1	BOOL	Status

FIG. 17

	Offset	Size in bytes	Data Type	Value
1800	0 to 3	4	UINT	PDS_RQ_READSECTOR
1810	4	1	BYTE	
1820	5 to 8	4	DWORD	
1830	9 to 12	8	LONGLONG	

FIG. 18

	Offset	Size in bytes	Data Type	Value
1900	0 to 3	4	UINT	PDS_RES_READSECTOR
1910	4 to 7	4	UINT	
1920	8 to 11	4	UINT	
1930	12 to 20	8	LONGLONG	
1940	21 to -		BYTE	

FIG. 19

	Offset	Size in bytes	Data Type	Value
2000	0 to 3	4	UINT	PDS_RQ_CHGENCRYPT
2010	4	1	BOOL	
2020	5	40	BYTE	

FIG. 20

	Offset	Size in bytes	Data Type	Value
2100	0 to 3	4	UINT	PDS_RES_CHGENCRYPT
2110	4	1	BOOL	Encryption

FIG. 21

	Offset	Size in bytes	Data Type	Value
2200	0 to 3	4	UINT	PDS_RQ_TERMINATE

FIG. 22

	Offset	Size in bytes	Data Type	Value
2300	0 to 3	4	UINT	PDS_RES_TERMINATE
2310	4	1	BOOL	

FIG. 23

	Offset	Size in bytes	Data Type	Value
2400	0 to 3	4	UINT	
2410	4	1	BYTE	

FIG. 24

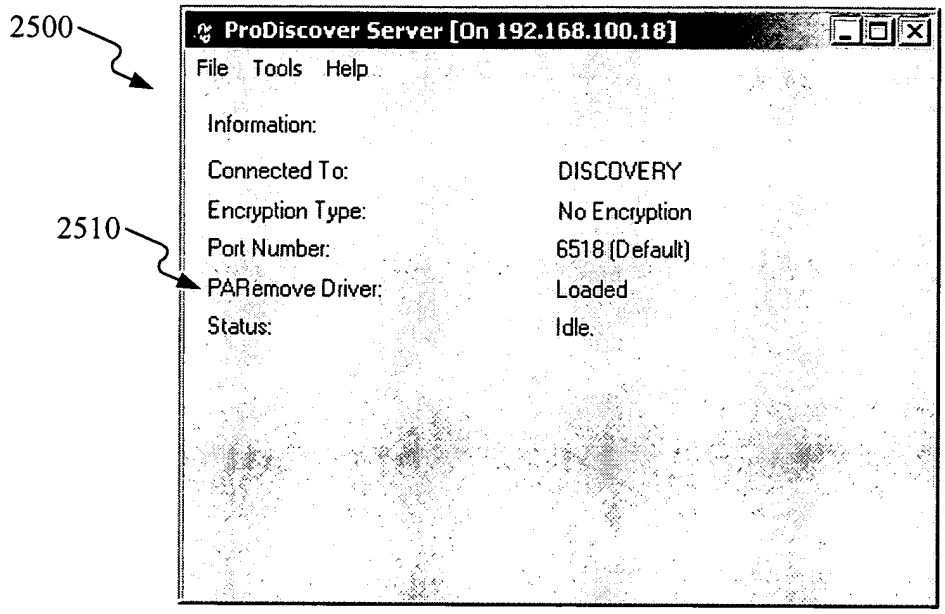
2500
ProDiscover Server [On 192.168.100.18]
File Tools Help
Information:
Connected To: DISCOVERY
Encryption Type: No Encryption
2510
Port Number: 6518 (Default)
PARemove Driver: Loaded
Status: Idle.

FIG. 25

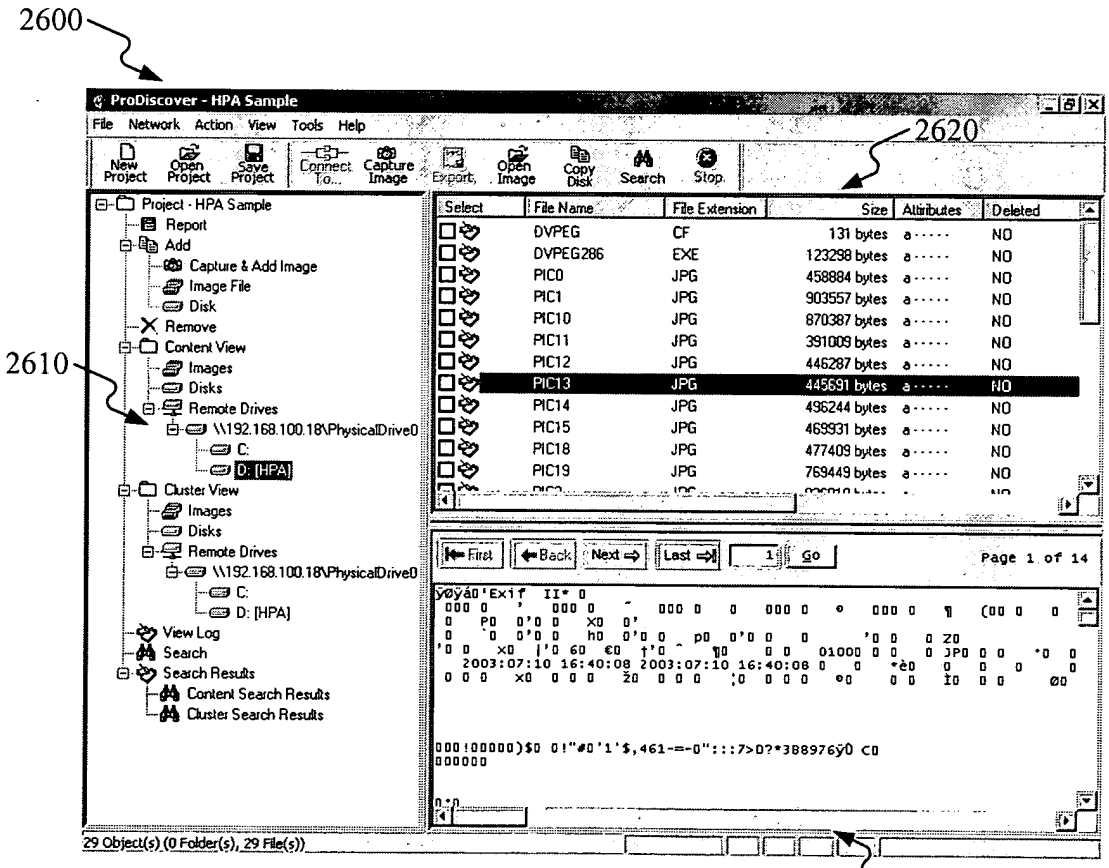
2600
ProDiscover - HPA Sample
File Network Action View Tools Help
New Project
Open Project
Save Project
Connect To...
Capture Image
Export
Open Image
Copy Disk
Search
Stop
2620
2610
Project - HPA Sample
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Disks
Remote Drives
\\192.168.100.18\PhysicalDrive0
C:
D: [HPA]
Cluster View
Images
Disks
Remote Drives
\\192.168.100.18\PhysicalDrive0
C:
D: [HPA]
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Select
File Name
File Extension
Size
Attributes
Deleted
DVPEG CF 131 bytes a····· NO
DVPEG286 EXE 123298 bytes a····· NO
PIC0 JPG 458884 bytes a····· NO
PIC1 JPG 903557 bytes a····· NO
PIC10 JPG 870387 bytes a····· NO
PIC11 JPG 391009 bytes a····· NO
PIC12 JPG 446287 bytes a····· NO
PIC13 JPG 445691 bytes a····· NO
PIC14 JPG 496244 bytes a····· NO
PIC15 JPG 469931 bytes a····· NO
PIC18 JPG 477409 bytes a····· NO
PIC19 JPG 769449 bytes a····· NO
First
Back
Next
Last
Go
Page 1 of 14
29 Object(s) (0 Folder(s), 29 File(s))
2630

FIG. 26